A simple and short proof of Fermat's last theorem for $n = 3$

A.M.D.M.Shadini , R.A.D.Piyadasa
Department of mathematics,University of Kelniya,Kelamiya

ABSTRACT

The first proof of Fermat's last theorem for the exponent $n = 3$ was given by Leonard Euler. However, Euler did not establish in full the key lemma required in the proof [1]. Since then, several authors have published proof for the cubic exponent but Euler's proof may have been supposed to be the simplest. Ribenboim [1] claims that he has patched up Euler's proof and Edwards [2] also has given a proof of the critical and key lemma of Euler's proof using the ring of complex numbers. Recently, Macys [3] in his article, claims that he may have reconstructed Euler are proof by providing an elementary proof for the key lemma. However, in this authors' point of view, none of these proofs is short nor easy to understand compared to the simplicity of the wording and the meaning of the theorem.The main objective of this paper is, therefore, to provide a simple and short proof for the theorem. It is assumed that the equation $z^3 = y^3 + x^3, \quad (x, y) = 1$ has non-trivial integer solutions for (x, y, z). Parametric solution of x, y, z and a necessary condition that must be satisfied by the parameters can be obtained using elementary mathematics. The necessary condition is obtained and the theorem is proved by showing that this necessary condition is never satisfied.

Proof of the theorem

The necessary condition satisfied by the parameters is obtained using following simple lemmas assuming that x, y, z satisfy the Fermat equation

$$z^3 = y^3 + x^3, (x, y) = 1 \tag{1}$$

and showing that one of x, y, z divisible by 3.

Lemma. 1

If $a^3 \equiv b^3 (\bmod 3^m) \quad (m \neq 0)$ and $(a,3) = (b,3) = 1$ then $a \equiv b (\bmod 3^{m-1})$ and $m \geq 2.$

If we assume that $a^3 - b^3 = 3^{3m} t^3$ and $(a, b) = 1$ in addition to $(a,3) = (b,3) = 1$, then $a - b = 3^{3m-1} u^3$, where u is a factor of t.

Proof:

$$F(a, b) = a^3 - b^3 = (a - b)[(a - b)^2 + 3ab]$$

(2)

and it follows from (2) that $a \equiv b (\bmod 3^{m-1})$, $m \geq 2$ since the term in the closed bracket or $a - b$ is divisible by 3 ,and $(3, ab) = 1$.

Now, if we assume

$$a^3 - b^3 = 3^{3m} t^3 \tag{3}$$

we can write $a - b = 3^{3m-1} f_1$, where $(3, f_1) = 1$, and we obtain

$$3^{3m} t^3 = 3^{3m} f_1 (b^2 + 3^{3m-1} f_1 b + 3^{6m-3} f_1^2)$$

Since $a - b = 3^{3m-1} f_1, \quad (a, b) = 1$, we conclude that $(f_1, b) = 1$. Hence, f_1 is a cube and let $f_1 = u^3$, which completes the proof of the Lemma.1.

Lemma.2

If the equation (1) has an integral solution (x, y, z) then one of x, y, z is divisible by 3.

Proof:

Using

$$z^3 = x^3 + y^3 = (x+y)^3 - 3xy(x+y) \tag{4}$$

and

$$(x+y-z)^3 = (x+y)^3 - 3(x+y)^2 z + 3(x+y)z^2 - z^3 \tag{5}$$

we obtain

$$(x+y-z)^3 = 3(x+y)(z-y)(z-x) \tag{6}$$

Since

$$(x+y)-z = x-(z-y) = y-(z-x) \tag{7}$$

factors common to $x+y-z$ and x, y, z are factors of $z-y, z-x$ and $x+y$ respectively. Hence, we deduce from (6) that one of x, y, z is divisible by 3.

If we assume y is divisible by 3, then

$$z - x = 3^{3m-1}u^3 \tag{8}$$

Since $3(z-x)$ is a cube, $z-y, x+y$ are also cubes and let $z-y=h^3$ and $x+y=g^3$. Then $2(x+y-z) = x+y-(z-x)-(z-y)$ and we obtain

$$2.3^m ugh = g^3 - 3^{3m-1}u^3 - h^3 \tag{9}$$

where $h, 3^m u, g$ are factors of x, y, z respectively. These parameters must satisfy

$$g^3 - h^3 - 2.3^m ugh - 3^{3m-1}u^3 = 0 \tag{10}$$

Our assumption that y is divisible by 3 is quite general since x, y, z in (1) can be replaced by $-x, -y, -z$. Since (10) is a cubic in g, g must have a real root if we fix m, u in (10) and solve it for the real root of g for different h, the factor of x. It follows from (10) and the Lemma.1 that

$$g - h = 3^{m-1} j \qquad (m \geq 2)$$ (11) unless $uh \neq 0$.

From (10), we obtain

$$h^3 + 3^{3m-1}u^3 = (h + 3^{m-1}j)\left[(h+3^{m-1}j)^2 - 2.3^m uh\right] \tag{12}$$

Since we are looking for g for different h, treating the left hand side of the equation as a function of h, we must have

$$(-3^{m-1}j)^3 + 3^{3m-1}u^3 = 0$$

i.e. $$3^2 u^3 = j^3$$

Since $(3, j) = 1$, this is never satisfied and we deduce that the equation (1) has no non-trivial solution for x, y, z.

References

(1) H.M.Edwards, Fermat's last theorem, A Genetic Introduction to Algedraic Number Theory, Spinger-Verlag, 1977.

(2) P.Ribenboim, Fermat's last theorem for amateurs, Springer-Verlag, New York, 1999.

(3) J,J.Macys, On Euler's Hypothetical Proof, Math, Notes.(3) 82(2007),352-356.